

LES ASSOCIATIONS
&
LE RÈGLEMENT GÉNÉRAL SUR LA
PROTECTION DES DONNÉES
RGPD



CONTEXTE

Qu'est-ce que le Règlement Général sur la Protection des Données ?

1

Un règlement européen responsabilisant les organisations pour qu'elles protègent les données personnelles qu'elles détiennent.

2

Une loi qui est entrée en application en France le 25 mai 2018

3

Un moyen pour tous les citoyens de l'Union Européenne **de reprendre le contrôle de leurs données personnelles**

Qu'est-ce qu'une donnée personnelle

Une donnée à caractère personnel est une information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement.

Identifiants

NOM, PSEUDO, OU
IDENTIFIANT EN LIGNE,
ADRESSE MAIL, POSTALE,
NUMÉRO DE TÉLÉPHONE,
DONNÉE DE LOCALISATION
...

Éléments identitaires

PHYSIQUES,
PHYSIOLOGIQUES,
GÉNÉTIQUES, PSYCHIQUES
...

Éléments sociétaux

ÉCONOMIQUES, CULTURELS,
SOCIAUX
...



Quelles associations sont concernées

TOUTES ! OU PRESQUE

1

A partir du moment où elles collectent (ex : avec un questionnaire), **stockent** (ex : sur un téléphone), **utilisent** (ex : en envoyant un mail) **des données à caractère personnel.**

2

Dès qu'elles traitent des données personnelles des différentes communautés avec lesquelles elles échangent : adhérents, bénévoles, donateurs, partenaires, bénéficiaires, salariés, etc.

3

Les sanctions en cas de non respect sont : limitation temporaire ou définitive d'un traitement, suspension des flux de données, ordre d'effacer les données, amendes jusqu'à 20 millions d'euros, etc.

ÉTAPES ET POINTS D'ATTENTION

ETAPE N°1

DÉSIGNER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)



Choisir une personne qui :

- sera le “chef d’orchestre” de la mise en place de la RGPD au sein de l’association
- est volontaire
- a des connaissances en informatique, en sécurité en ligne, juridique, nouvelles technologies de l’information et de la communication (NTIC).



CONSEIL :

Si vous ne comptez personne avec de telles compétences dans votre structure, tournez-vous vers vos bénévoles, adhérents, etc. ou vers un acteur de l’accompagnement associatif pour vous aider dans les démarches à suivre.

ETAPE N°1

QUEL EST LE RÔLE DU DPO ?



Ses missions :

S'assurer que son organisation respecte la législation lorsqu'elle utilise les données à des fins externes et internes :

- informer et conseiller les membres de l'association
- contrôler le respect du règlement en matière de protection des données
- coopérer avec l'autorité de contrôle et être le point de contact de celle-ci
- s'informer sur le contenu des nouvelles obligations
- réaliser l'inventaire des traitements de données de l'association
- concevoir des actions de sensibilisation
- piloter la conformité en continu.

ETAPE N°2

FAIRE UN ÉTAT DES LIEUX DE VOTRE TRAITEMENT DES DONNÉES



Cartographier les données personnelles détenues par l'association

Les questions à se poser :

- 1. Quelles sont les données personnelles détenues ?
 - nom, prénom
 - adresse mail, postale
 - diverses informations personnelles...
- 2. Quels en sont les modes d'acquisition ?
 - inscription en ligne
 - carte de visite
 - par téléphone...
- 3. Où sont-elles hébergées, conservées, archivées ?
 - sur ordinateur
 - sur un logiciel
 - sur un téléphone...

ETAPE N°2

FAIRE UN ÉTAT DES LIEUX DE VOTRE TRAITEMENT DES DONNÉES



Cartographier les données personnelles détenues par l'association

Les questions à se poser :

- 4. Quelle utilisation avez-vous de ces données ?
 - appels aux dons
 - invitation à des événements
 - aides bénévoles

- 5. Qui a accès à ces données et comment ?
 - tout le monde, il n'y a pas de protection
 - **x** le département de l'administration à l'aide **✓** d'un code d'accès, etc.

- 6. Quelle est la durée de conservation de ces données ?
 - depuis l'enregistrement de la donnée
 - depuis 3 ans, etc. **✓**

ÉTAPE N°3

METTRE EN PLACE UN PLAN D'ACTION POUR ÊTRE EN RÈGLE



Un plan d'action pour quelles données et quels traitements ?

Suite à l'état des lieux des données personnelles détenues par l'association et à la réalisation du registre reprenant tous les éléments, 3 champs d'actions s'offrent à vous :

1. **Trier les données personnelles détenues par l'association**
2. **Respecter les droits des personnes sur leurs données personnelles**
3. **Sécuriser les données personnelles détenues par l'association.**

1. TRIER LES DONNÉES PERSONNELLES DÉTENUES PAR L'ASSOCIATION

- ❑ S'assurer que **seules les données strictement nécessaires** à l'action de l'association sont collectées et traitées.
- ❑ Conserver les données uniquement pour une **durée nécessaire et respectant les droits** (3 ans dans la majorité des cas).
- ❑ Vérifier de **ne traiter aucune donnée dite « sensible »*** ou, si c'est le cas, être sûr d'avoir le droit de les traiter.
- ❑ Contrôler que seules les **personnes habilitées** ont accès aux données dont elles ont besoin.



CONSEIL :

N'hésitez pas à supprimer des données anciennes.

Les personnes qui souhaitent revenir vous voir trouveront toujours le chemin !

*CNIL : information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

2. RESPECTER LES DROITS DES PERSONNES SUR LEURS DONNÉES PERSONNELLES (1/2)

Pour les données personnelles que l'association détient déjà...

L'association doit :

- ❑ informer (sur son site internet, par mail, par téléphone) les personnes concernées qu'elle détient des données personnelles à leur sujet
- ❑ leur demander si elles souhaitent que l'association les conserve (si oui lesquelles)
- ❑ supprimer, actualiser ou conserver les données personnelles.



CONSEIL :

Si vous communiquez des données hors de l'Union européenne, précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données.

2. RESPECTER LES DROITS DES PERSONNES SUR LEURS DONNÉES PERSONNELLES (2/2)

Pour les nouvelles données personnelles que l'association collecte, sur le support utilisé (formulaire, etc.), l'association doit faire figurer :

L'association doit :

- ❑ pourquoi ces données sont collectées « la finalité »,
- ❑ ce qui l'autorise à traiter ces données « fondement juridique » et/ou « intérêt légitime »,
- ❑ qui a accès aux données,
- ❑ combien de temps elle les conserve,
- ❑ les modalités selon lesquelles les personnes peuvent exercer leurs droits (en cliquant sur un lien de désinscription, par mail, par un courrier postal).

3. SÉCURISER LES DONNÉES PERSONNELLES DÉTENUES PAR L'ASSOCIATION

- ❑ Identifier la **base juridique** sur laquelle se fonde le traitement de la donnée (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale)
- ❑ Réviser les **mentions d'information** afin qu'elles soient conformes aux exigences du règlement (articles 12, 13 et 14 du règlement)
- ❑ Prévoir les **modalités d'exercice** des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...)
- ❑ Vérifier les **mesures de sécurité** mises en place : codes, clés, accès, etc.

ETAPE N°4

DÉFINIR DES PROCESSUS ET CRÉER DE LA DOCUMENTATION

Cartographier les données personnelles détenues par l'association

Après avoir mis en place le plan d'actions pour respecter la RGPD, définir des processus et documenter permet de capitaliser sur le travail réalisé et de prouver la conformité.

La rédaction et la mise en place des processus permet :

- ❑ de prendre en compte la protection des données personnelles dès la conception du traitement de celles-ci
- ❑ de sensibiliser et d'organiser la remontée d'information en construisant notamment un plan de formation et de communication auprès de vos collaborateurs
- ❑ de traiter plus facilement et rapidement les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits.

ETAPE N°4

DÉFINIR DES PROCESSUS ET CRÉER DE LA DOCUMENTATION

Cartographier les données personnelles détenues par l'association

Après avoir mis en place le plan d'actions pour respecter la RGPD, définir des processus et documenter permet de capitaliser sur le travail réalisé et de prouver la conformité.

La constitution d'une documentation comprend par exemple :

- le registre
- le plan d'action avec le rétroplanning
- les processus mis en place avec les responsabilités de chacun.

A young boy in a blue shirt and dark shorts is running on a paved path in a park. A large, leafy tree is in the background. The scene is captured in a slightly blurred, dynamic style.

ALLER PLUS LOIN

DES RESSOURCES COMPLÉMENTAIRES

Pour approfondir :

- ★ Une vidéo du [Journal du Net](#)
- ★ Une vidéo du youtubeur [Cookie connecté](#)
- ★ Une [note du Mouvement Associatif](#) sous forme de FAQ.



QUELQUES CONSEILS POUR FINIR...



Bien définir les rôles avant de se lancer :

En prenant le temps de désigner le Délégué à la protection des données, faire un état des lieux clair sur les données personnelles détenues par l'association à l'aide d'un registre, vous serez ensuite davantage en mesure de mettre en place les actions.

Être transparent et informer :

La règle d'or est d'être le plus transparent possible avec les personnes dont l'association détient des données personnelles : les écouter, répondre à leurs demandes, leur montrer sa bonne intention, etc.



helloasso

agir ensemble